UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/747,759 | 12/21/2000 | Thomas A. Kean | 19546-020110US | 4704 |

34313 7590 07/25/2005

ORRICK, HERRINGTON & SUTCLIFFE, LLP
IP PROSECUTION DEPARTMENT
4 PARK PLAZA
SUITE 1600
IRVINE, CA 92614-2558

| EXAMINER | |
|---|---|
| JUNG, DAVID YIUK | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/747,759 | KEAN, THOMAS A. | |
| | Examiner | Art Unit | |
| | Jonathan R Adams | 2134 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *25 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8,9,11-13 and 18-111* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 6, 7, 10, and 14-17 have been cancelled.

2. Claims 30 and 42 have been amended.

3. Claims 56-111 have been added.

### *Response to Arguments*

4. Applicant's arguments filed 12/28/04 have been fully considered but they are not persuasive.

5. In response to the applicant's arguments stating that the Garnett reference teaches that the configuration data is encrypted outside the FPGA and this is contrary to the applicant's invention, the examiner disagrees. As broadly as stated in the claims, the security circuit merely corresponds to the integrated circuit and is not necessarily held within, and is therefore taught by the embodiment taught by Garnett.

6. In response to the applicant's arguments stating that the security algorithms taught by secondary references are impossible to implement on an FPGA, the applicant has provided no evidence as to the validity of the argument, and will therefore be disregarded until such evidence is provided.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was

within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Applicant's arguments with respect to claims 46-55 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 112***

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 30, 42, 54, and 55 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. As to claim 30:

The term "high" used in "High voltage" is a relative term rendered indefinite for having no comparative reference.

4. As to claim 42

Claim 42 recites the limitation "the configured user logic" in line 1. There is insufficient antecedent basis for this limitation in the claim.

5. As to claim 54:

The limitation "about a microamp or less" renders the claim indefinite for failing to distinctly claim the range of current draw.

6. As to claim 55:

The limitation "about 10 microamps or less" renders the claim indefinite for failing to distinctly claim the range of current draw.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

8. Claims 1, 3, 4, and 5 rejected under 35 U.S.C. 102(a) as being anticipated by Garnett, US Patent No 6356637 (hereafter referred to as '637).

9. As to claim 1:

'637 teaches a FPGA configuration system using encrypted configuration data comprising:

- Inputting a stream of data comprising unencrypted configuration data to the integrated circuit / Inputting configuration data (Col 2, Line 33, '637)
- encrypting the unencrypted configuration data / Encrypting the configuration data (Col 2, Line 34, '637)
- using a security circuit and a security key / Encryption algorithm utilizes an encryption key (Col 2, Line 38, '637)
- outputting a stream of encrypted configuration data / inputting encrypted configuration data into the FPGA [from encryption logic] (Col 2, Line 46, '637)

10. As to claim 3:

Configuring the integrated circuit using the unencrypted configuration data / distributing the decrypted configuration data to configure the FPGA (Col 2, Line 48, '637)

11. As to claim 4:

Storing the stream of encrypted configuration data in a nonvolatile storage device / Flash PROMs ... easily configure an FPGA (Col 1, Line 6, XPFSP)

12. As to claim 5:

Inputting the stream of encrypted configuration data / inputting encrypted configuration data into the FPGA [from encryption logic] (Col 2, Line 46, '637)

***Claim Rejections - 35 USC § 103***

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 2 and 21-24 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of Xilinx Programmable FLASH Serial PROMs (hereafter referred to as XPFSP).

As to claim 2:

15. '637 teaches a FPGA configuration system using encrypted configuration data. '637 does not specifically teach for the configuration data to be input serially. XPFSP teaches an FPGA system\device using many specific device attributes including serial transfer of configuration data (Col 1, Line 6 et seq., XPFSP). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the FPGA system\device of XPFSP with the encrypted configuration system of '637. One of ordinary skill in the art would have been motivated to use the FPGA system\device of XPFSP with the encrypted configuration system of '637 because using serial communications for the transfer of configuration data reduces used chip pin count and reduces circuit complexity.

16. As to claim 21:

Receiving the stream of encrypted configuration data using a microprocessor / in '637 as modified above, the storage device of XPFSP receives configuration data using a cryptography processor

17. As to claim 22 - 24:

using the microprocessor, writing the encrypted configuration data into a nonvolatile storage device / nonvolatile storage device is a serial EPROM or serial EEPROM / nonvolatile storage device is a Flash memory / Flash programmable PROM (Col 1, Line 2, XPFSP)

18. Cancelled claims 6, 7, and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of TCP/IP security.

As to cancelled claims 6, 7, and 14:

19. '637 as modified above teaches a FPGA configuration system using encrypted configuration data. '637 as modified above does not teach for the configuration data packet to have an encryption header for determining if the configuration data packet is encrypted. TCP/IP security teaches a packet communications system using a packet header comprising sub-headers to determine if and how the data packet is encrypted (Page 21, Line 5, TCP/IP security). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the encryption packet header system of TCP/IP security with the encrypted configuration data communication of '637. One of ordinary skill in the art would have been motivated to use the encryption packet header

system of TCP/IP security with the encrypted configuration data communication of '637 because using a packet header to determine packet data content characteristics is the standard method and provides simple reliable means for coordinating encryption protocol specifics.

20. Claims 8, 12, and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of TCP/IP security in further view of Bruce Schneier, Applied Cryptography (hereafter referred to as Schneier).

As to claim 8:

21. '637 as modified above teaches a FPGA configuration system using encrypted configuration data and cryptographic keys. '637 as modified above does not teach that keys should be generated with a random number generator. Schneier teaches key management techniques including key generation stating, "good keys are random-bit strings generated by some automatic process" (Page 173, Line 17, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use a random number generator to generate cryptographic keys. One of ordinary skill in the art would have been motivated to use a random number generator to generate cryptographic keys because perfectly random keys are the hardest keys to be broken by cryptanalysis.

As to claim 12:

22. '637 as modified above teaches a FPGA configuration system using encrypted configuration data. '637 as modified above does not teach for the unencrypted configuration data has approximately the same number of bits as the encrypted configuration data. Schneier teaches general cryptographic foundations including that with some algorithms the ciphertext is the same size as the original plaintext message (Page 2, Line 7, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use an encryption algorithm where the produced ciphertext would have approximately the same number of bits as the plaintext. One of ordinary skill in the art would have been motivated to use an encryption algorithm where the produced ciphertext would have approximately the same number of bits as the plaintext because it would represent the minimum data size without first compressing the configuration data.

As to claim 35:

23. '637 as modified above teaches a FPGA configuration system using encrypted configuration data with a cryptographic processor implementing DES and CBC mode (Col 6, Line 17, '286). '637 as modified above does not teach to use triple DES. Schneier teaches the use of triple DES to heighten algorithm security (Page 359, Line 9, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use triple DES with the cryptographic processor in the invention of '637 as modified above. One of ordinary skill in the art would have been motivated to use

triple DES with the cryptographic processor in the invention of '637 as modified above because triple encryption helps improve security.

24. Claims 9, 11, 13, 19, 25-29, 32-34, and 36 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of TCP/IP security in further view of Schneier in further view of Pastor et al., US Patent No 4878246, (hereafter referred to as '246).

As to claims 9, 11, and 13:

25. '637 as modified above teaches a FPGA configuration system using encrypted configuration data and cryptographic keys stored in non-volatile registers. '637 as modified above does not teach for the keys to be associated with the device ID. '246 teaches a cryptographic communications system using a generation of cryptographic keys based on an identification number. It would have been obvious to a person of ordinary skill in the art at the time of invention to seed the cryptographic key with the device identification as in '246 in the invention of '637. One of ordinary skill in the art would have been motivated to seed the cryptographic key with the device identification as in '246 with the invention of '637 because the possibility that the key may be generated by unauthorized personnel unaware of the identification number would be substantially reduced (Col 1, Line 8, '246).

26. As to claim 19:

Stream of data is loaded using a JTAG interface of the integrated circuit / Reprogrammed using the JTAG port and then the bit stream is downloaded to the FPGA (Col 1, Line 1, XPFSP)

As to claims 25-27 and 29:

27. '637 as modified above teaches a FPGA configuration system using encrypted configuration data using flash memory, fusible link PROM, UV-EPROM, OTPROM, ferroelectric cells, and laser programmable fuses for storing data device ID/key data (Col 5, Line 25 et seq., '637). '637 as modified above does not explicitly teach for the device ID/Key to be stored on other types of non volatile memory such as floating-gate transistors and antifuses. The examiner takes official notice as to use antifuses and floating-gate transistors as a nonvolatile memory alternatives. It would have been obvious to a person of ordinary skill in the art at the time of invention to use antifuses and floating-gate transistors as a nonvolatile memory alternatives because antifuses and floating-gate transistors represent functionally equivalent nonvolatile memory alternatives.

28. As to claim 28:

ID register is programmed during manufacture of the integrated circuit / decryption key storage is loadable with the decryption key at the manufacturing stage (Col 5, Line 33, '637)

29. As to claim 32:

- security key has a fixed value / decryption key storage is loadable with the decryption key at the manufacturing stage (Col 5, Line 33, '637)
- generating an initial value for the security circuit / cryptographic keys based on an identification number (Col 1, Line 7, '246)
- outputting the initial value / it is inherent to the '637 as modified above that during the manufacturing stage an integrated circuit must output the initial value for it to be loaded into the decryption key storage

30. As to claim 33:

unencrypted configuration data is encrypted using the initial value / Encrypting the configuration data (Col 2, Line 34, '637)

31. As to claim 34:

initial value is generated using a random number generator / "good keys are random-bit strings generated by some automatic process" (Page 173, Line 17, Schneier)

As to claim 36:

32. '637 as modified above teaches a FPGA configuration system using encrypted configuration data using a Device ID/key register to store the Device ID/key. '637 as modified above does not teach for the Device ID register to be implemented using an error correcting code scheme. Schneier teaches a key error detection techniques used to protect cryptographic keys (Page 178, Line 33 et seq,. Schneier). It would have been

obvious to a person of ordinary skill in the art at the time of invention to use the key error detection techniques listed in Schneier with the invention of '637 as modified above. One of ordinary skill in the art would have been motivated to use the key error detection techniques listed in Schneier with the invention of '637 as modified above because using key error detection can prevent the generation of garbled and undecipherable text.

33. Claim 30 (claims 10, 15-17 cancelled) rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of TCP/IP security in further view of Schneier in further view of '246 in further view of Xilinx XC4000.

Claim 10 (cancelled):

34. '637 as modified above teaches a FPGA configuration system using encrypted configuration data messages and encryption and authentication message header preambles (Page 21, Fig 12, XPFSP). '637 as modified above does not specifically teach that the configuration data should comprise preamble, header, and initial value. Xilinx teaches an FPGA with configuration data further comprising Initial value / Start Field (Page 166, Table 9, Xilinx). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the Xilinx FPGA configuration data with the secure FPGA configuration system of '637 as modified above. One of ordinary skill in the art would have been motivated to use the Xilinx FPGA configuration data with the secure FPGA configuration system of '637 as modified above because the Xilinx FPGA

is one of the most readily available FPGAs on the market and is a standard for compatibility.

35. Claim 15 (cancelled)

Integrated circuit can determine whether the stream of data is for a previous version of without a security scheme / Authentication Header and Encryption Header serve as security options (Page 18, Line 1, TCP/IP Security)

36. Claim 16 (cancelled):

A integrated circuit with a security scheme will be backwards compatible with versions of the integrated circuit without the security scheme / Authentication Header and Encryption Header serve as security options (Page 18, Line 1, TCP/IP Security)

37. Claim 17 (cancelled):

Processing the stream of data based on preamble value determining security scheme / See rejection for claim 6

38. As to claim(s) 30:

'637 as modified above teaches a FPGA configuration system using encrypted configuration data using flash memory. '637 as modified above does not specifically teach the voltage requirements for proper configuration. Xilinx XC4000 teaches the use of the proper electrical requirements for the device. It would have been obvious to a

person of ordinary skill in the art at the time of invention to use the correct programming voltage to ensure proper configuration as taught by Xilinx XC4000. One of ordinary skill in the art would have been motivated use the correct programming voltage to ensure proper configuration as taught by Xilinx XC4000 because electrical components all have specified operating voltages which should be followed to ensure proper configuration and prevent damage to the device.

39. Claims 18 and 31 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of TCP/IP security in further view of Schneier in further view of '246 in further view of Xilinx XC4000 in further view of Roselli, US Patent No 5036468 (hereafter referred to as '468).

As to claim 18:

40. '637 as modified above teaches a FPGA configuration system using encrypted configuration data storing security key in nonvolatile memory. '637 as modified above does not teach the use of an external battery to backup the power supply. '512 teaches using an external battery to backup the power supply (Col 2, Lines 50-53, '512). It would have been obvious to a person of ordinary skill in the art at the time of invention to use an external battery to backup the main power supply as done in '512 in the invention of '637 as modified above. One of ordinary skill in the art would have been motivated to use an external battery to backup the main power supply as done in '512 in the invention of '637 as modified above because using a battery backup for the main

power supply guaranties memory retention and operation in the event of a power outage.

41. As to claim 31:

external battery is coupled to a first power supply terminal to the ID register, and a second power supply terminal for non-backed up circuits is not coupled to the external battery / battery (Fig 1, Element 10, '512), real time clock (Fig 1, Element 12, '512)

42. Claim 20 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of Lai et al, US Patent No 6324286 hereafter referred to as '286.

As to claim 20:

43. '637 as modified above teaches a FPGA configuration system using encrypted configuration data. '637 does not specifically teach the processing means to encrypt the configuration data. '286 teaches a cryptographic processor for encrypting and outputting data in several possible modes. It would have been obvious to a person of ordinary skill in the art at the time of invention to use a cryptographic processor as in '286 for the encryption and output of configuration data. One of ordinary skill in the art would have been motivated to use a cryptographic processor as in '286 for the encryption and output of configuration data because encryption must be accomplished by some processing means, and cryptographic processors provide a specialized efficient method for encryption.

44. Claim 37, 38, 42, and 43 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of Hair, US Patent No 6615349 (hereafter referred to as '349).

As to claim 37:

'637 teaches a FPGA configuration system using encrypted configuration data comprising:

- Inputting a stream of data comprising unencrypted configuration data to the integrated circuit / Inputting configuration data (Col 2, Line 33, '637)
- encrypting the unencrypted configuration data / Encrypting the configuration data (Col 2, Line 34, '637)
- using a security circuit and a security key / Encryption algorithm utilizes an encryption key (Col 2, Line 38, '637)
- outputting a stream of encrypted configuration data / inputting encrypted configuration data into the FPGA [from encryption logic] (Col 2, Line 46, '637)

45. '637 does not teach to first obtain the file from a network employing an encrypted communications channel. '349 teaches a secure communication system that retrieves a file from the internet using cryptographic communications (Col 20, Line 25 et seq., '349). It would have been obvious to a person of ordinary skill in the art at the time of invention to retrieve the file over the Internet using cryptographic communications as in '349 in the invention of '637. One of ordinary skill in the art would have been motivated to retrieve the file over the Internet using cryptographic communications as in '349 in the invention

of '637 because doing so helps to "prevent unauthorized use of replication of the computer files or programs" (Col 5, Line 6, '349).

46. As to claim 38:

outputting a stream of encrypted configuration data / inputting encrypted configuration data into the FPGA [from encryption logic] (Col 2, Line 46, '637)

47. As to claim(s) 42:

User programmed circuitry outputs the unencrypted configuration data to the security circuit using an on-chip interconnection / FPGA also includes configuration data decryption circuitry in the form of logic and memory for data received through communication link 10 (Col 5, Lines 10-13, '637), key data defining the operand is loadable from the memory into the logic through a communication link 16 (Col 5, Lines 22-24, '637)

48. As to claim 43:

Configuring the integrated circuit using the unencrypted configuration data / distributing the decrypted configuration data to configure the FPGA (Col 2, Line 48, '637)

49. Claim 39, 40, and 44 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of '349 in further view of XPFSP.

As to claims 39 and 44:

50. '637 as modified above teaches a FPGA configuration system using encrypted configuration data retrieved from a network using cryptographic communications. '637 as modified above does not specifically teach for the configuration data to be input serially from a nonvolatile storage device. XPFSP teaches an FPGA system\device using many specific device attributes including storing configuration data in a nonvolatile storage device (Col 1, Line 6, XPFSP). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the FPGA system\device of XPFSP with the encrypted configuration system of '637. One of ordinary skill in the art would have been motivated to use the FPGA system\device of XPFSP with the encrypted configuration system of '637 because it is the standard convention to configure FPGAs from nonvolatile storage devices.

51. As to claim 40:

Nonvolatile storage device is serial EPROM / Programmable FLASH serial PROMs (Page 21, XPFSP)

52. Claims 41 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of '349 in further view of XPFSP in further view of '246.

As to claims 41:

53. '637 as modified above teaches a FPGA configuration system using encrypted configuration data and cryptographic keys stored in non-volatile registers. '637 as modified above does not teach for the keys to be associated with the device ID. '246

teaches a cryptographic communications system using a generation of cryptographic keys based on an identification number. It would have been obvious to a person of ordinary skill in the art at the time of invention to seed the cryptographic key with the device identification as in '246 in the invention of '637. One of ordinary skill in the art would have been motivated to seed the cryptographic key with the device identification as in '246 with the invention of '637 because the possibility that the key may be generated by unauthorized personnel unaware of the identification number would be substantially reduced (Col 1, Line 8, '246).

54. Claims 45 rejected under 35 U.S.C. 103(a) as being unpatentable over

As to claim 45:

55. '637 as modified above teaches a FPGA configuration system using encrypted configuration data. '637 does not specifically teach the processing means to encrypt the configuration data. '286 teaches a cryptographic processor for encrypting and outputting data in several possible modes. It would have been obvious to a person of ordinary skill in the art at the time of invention to use a cryptographic processor as in '286 for the encryption and output of configuration data. One of ordinary skill in the art would have been motivated to use a cryptographic processor as in '286 for the encryption and output of configuration data because encryption must be accomplished by some processing means, and cryptographic processors provide a specialized efficient method for encryption.

56. '637 as modified above teaches a FPGA configuration system using encrypted configuration data with a cryptographic processor implementing DES and CBC mode (Col 6, Line 17, '286). '637 as modified above does not teach to use triple DES. Schneier teaches the use of triple DES to heighten algorithm security (Page 359, Line 9, Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use triple DES with the cryptographic processor in the invention of '637 as modified above. One of ordinary skill in the art would have been motivated to use triple DES with the cryptographic processor in the invention of '637 as modified above because triple encryption helps improve security.

57. Claim 46-53 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 in view of XPFSP in further view of '349 in further view of '286 in further view of Schneier in further view of TCP/IP security in further view of '246 in further view of Xilinx XC4000 in further view '512.

58. As to claims 46-53:

Claims 46-53 correspond to claims 1-45 in various concomitant elements and are rejected accordingly.

59. Claim 55-90, 96-111 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 as modified for claims 46-53 in further view of Massoud Pedram, "Design Considerations for Battery-Powered Electronics".

60. As to claim(s) 54, 55

'637 as modified above teaches a FPGA configuration system using configuration data stored in a nonvolatile memory with an external battery backup. '637 as modified above does not teach the advantage of using low current draw for battery-powered electronics applications. Pedram teaches the advantages of using low current draw for battery-powered electronics applications (Page 1, Col 2, Line 5, Pedram). It would have been obvious to a person of ordinary skill in the art at the time of invention to use low current draw for the battery-powered electronics applications of '637 as modified above. One of ordinary skill in the art would have been motivated to use low current draw for the battery-powered electronics applications of '637 as modified above because low power design extends battery service time.

61. As to claims 56-90:

Claims 56-90 correspond to claims 1-45, 54-55 in various concomitant elements and are rejected accordingly.

62. Claims 96-111 correspond to claims 1-45, 54-55 in various concomitant elements and are rejected accordingly.

63. Claim 91-95 rejected under 35 U.S.C. 103(a) as being unpatentable over '637 as modified for claims 55-90 in further view of Choi, US Patent No 6233717 (hereafter referred to as '717)

64. As to claim(s) 91:

Claim 91 corresponds to claim 1 and further comprises:

'637 as modified above teaches a FPGA configuration system using configuration data stored in a nonvolatile memory utilizing an error detection protocol. '637 as modified above does not specifically teach for the error checking circuit to also perform error correction. '717 teaches a system for error detection and correction using a register of m bits (Memory cell array, Fig 1, Element 100, '717), error checking bits (Parity area, Fig 1, Element 160, '717) to perform error correction (Fig 1, Element 240, '717). It would have been obvious to a person of ordinary skill in the art at the time of invention to use an error correction/detection as in '717 in the invention of '637 as modified above. One of ordinary skill in the art would have been motivated to use an error correction/detection as in '717 in the invention of '637 as modified above because error correction schemes are in common use for correcting the inaccuracies of memory devices.

65. Claims 92-95 correspond to claims 1-45, 54-55 in various concomitant elements and are rejected accordingly.

***Conclusion***

66. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703)

305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

67. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100